UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

ANDREW AND SARAH FOSSUM, Plaintiffs v. **FIRST DATA CORPORATION,** Defendant	**Case No. 1:20-cv-00865** **JURY TRIAL DEMANDED**

COMPLAINT

Plaintiffs Andrew and Sarah Fossum ("Plaintiffs") hereby assert the following claims under the Electronic Funds Transfer Act, 15 U.S.C. §§ 1693, *et seq*. (the "EFTA") against Defendant First Data Corporation d/b/a Money Network and allege as follows:

THE PARTIES

1. Plaintiffs are residents of Travis County, Texas.

2. Defendant First Data Corporation ("First Data" or "Defendant"), also known as Fiserv, is a corporation organized and existing under the laws of the State of Texas that does business as Money Network in the State of Texas and in particular in Travis County.

3. Based on a complaint filed by the Federal Trade Commission (FTC), Defendant First Data has a concerning, recent history of "looking the other way" and thereby enabling fraud

via electronic fund transfers. First Data apparently settled the case for a substantial sum. On May 20, 2020, the FTC reported that "The FTC alleges that Atlanta-based First Data Merchant Services and its former vice president, Chi 'Vincent' Ko, engaged in conduct that helped scammers rake in megabucks at consumers' expense."[1] According to Daniel Kaufman, Deputy Director of the FTC's Bureau of Consumer Protection, "First Data is paying $40 million because it repeatedly looked the other way while its payment processing services were being used to commit fraud. When companies fail to screen out fraudsters exploiting the payment processing system to steal people's money, they're breaking the law – and injuring consumers."[2]

JURISDICTION AND VENUE

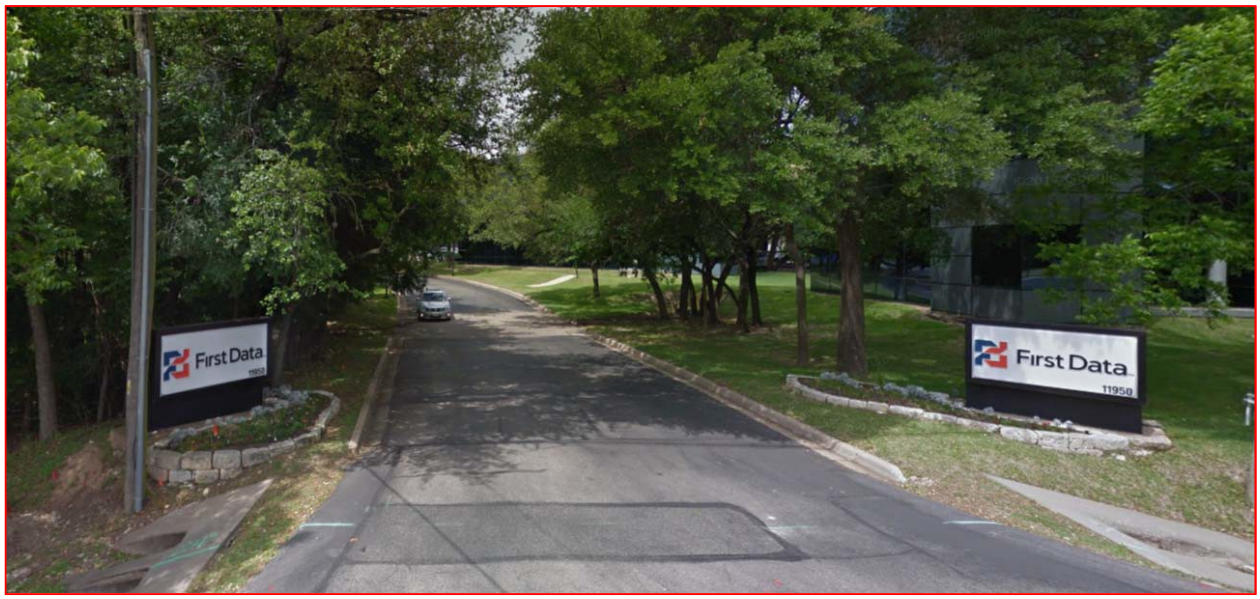
4. This action arises the federal Electronic Funds Transfer Act, 15 U.S.C. §§ 1693, *et seq*. (the "EFTA"). This Court has subject matter jurisdiction under 28 U.S.C. § 1331 and 15 U.S.C. § 1693m(g).

5. Venue in this district is proper under 28 U.S.C. § 1391(b)(1) and (c)(2) because First Data does business and maintains offices in this district. Venue in this district is also proper under 28 U.S.C. § 1391(b)(2) because a substantial part of the events giving rise to Plaintiffs' claims occurred in this district.

6. On information and belief, First Data maintains an office in Austin, Texas at 11950 Jollyville Road, Austin, Texas 78759.

7. The picture below shows the entrance to First Data's office at 11950 Jollyville Road, Austin, Texas 78759.

[1] See https://www.ftc.gov/news-events/blogs/business-blog/2020/05/402-million-reminder-about-importance-due-diligence.
[2] See https://www.ftc.gov/news-events/press-releases/2020/05/worldwide-payment-processor-payments-industry-executive-pay-402.



8. First Data's office at the above referenced location is a regular and established place of business of First Data.

BACKGROUND FACTS

9. Pursuant to the CARES Act, First Data was responsible for disbursing certain stimulus fund payments to United States citizens.

10. First Data, under its "Money Network" brand, disbursed certain of these stimulus fund payments by mailing debit cards to consumers. First Data referred to these cards as an "Economic Impact Payment Card" ("EIP Card").

11. On May 30, 2020, the US Postal Service ("USPS") delivered an EIP Card to Plaintiffs' address in Travis County, Texas.

12. Delivery of the EIP Card on May 30 was confirmed via the USPS website, which retains photographs of mail delivered on certain dates.

13. Sometime between delivery of the EIP Card on May 30 and early in the morning of May 31, 2020, all mail was stolen from Plaintiffs' mailbox.

14. During that same timeframe, mail was apparently stolen from neighborhoods surrounding Plaintiffs' neighborhood. On the morning of May 31, 2020, Plaintiffs' neighbor sent out an email to a community email group explaining that she had found a large bag of mail in the middle of the road. The mail was from Plaintiffs' community and other surrounding communities.

15. On May 31, 2020, after seeing the email about mail theft, Plaintiffs accessed the USPS website to see what mail had been stolen from the pictures that USPS provides. Based on this review and pictures of the envelopes containing EIP Cards available online, Plaintiffs determined that an envelope containing an EIP Card had been stolen along with other mail.

16. On May 31, 2020, that same day, Plaintiffs called First Data's customer service number, 1-800-240-8100, to report theft of the EIP Card.

17. During that call, Plaintiffs informed a customer service representative ("CSR") that the EIP Card had been stolen and the account should be frozen or otherwise disabled.

18. The CSR represented to Plaintiffs that the card would be reissued with a different account number.

19. The CSR provided Plaintiffs with the original EIP Card number and instructed Plaintiffs to call the automated customer service system, activate the card, and set a PIN number.

20. Plaintiffs followed the CSR's instructions.

21. Despite having been informed of the EIP Card theft, First Data apparently **did not** freeze, cancel, or otherwise disable the card.

22. On June 2 and June 3, 2020, an individual (or group of individuals) unknown to

Plaintiffs and without authorization made three fraudulent transfers from the card to a "Chime" bank account totaling $2,301.00.

23. Plaintiffs did not become aware of the June 2 and 3 transfers until June 9, 2020 as discussed below.

24. On June 8, 2020, Plaintiffs received the reissued EIP Card with a different account number and tried to use the card at an ATM. The card did not work.

25. On June 9, 2020, Plaintiffs tried, for the first time, to access the EIP Card website (www.eipcard.com) to create an account and to determine why the card was not working. Through the process of trying to create an account, it became clear that an account associated with the original EIP Card (which was supposed to have been disabled) had already been created by an individual (or group of individuals) unknown to Plaintiffs.

26. Because an account associated with the card had already been created and linked to an email account unknown to Plaintiffs, Plaintiffs called the customer support number for the EIP Card to determine what had happened. Plaintiffs first used the automated customer service system to check the balance of the card, which was $99 at that time.

27. After determining that the balance on the card was incorrect, Plaintiffs again called the customer service number and spoke to a CSR. The CSR assisted Plaintiffs with obtaining access to the EIP Card website by resetting the email address associated with the card account to an email address associated with Plaintiffs.

28. Once the email address had been changed, Plaintiffs were able to access the account information on the EIP Card website for the first time. That access permitted Plaintiffs to review the transfer history for the card and determine that transfers out of the EIP Card account had been made as described above.

29. Plaintiffs did not authorize the transfers, and Plaintiffs do not know the individual (or group of individuals) who made the transfers. Accordingly, Plaintiffs disputed the unauthorized transfers. Plaintiffs verbally informed First Data of these facts during the June 9 phone call.

30. During the same June 9 phone call discussed above and after obtaining access to the card account on the eipcard.com website, the CSR said that she could try to reverse the unauthorized charges. The CSR instructed Plaintiffs to call back in 7 business days (June 18) if the charges did not get reversed.

31. As of June 18, only a single charge of $2 had been reversed. As instructed, Plaintiffs called the customer service number again and spoke with another CSR. During that call Plaintiffs were informed that the charges could not be reversed, and Plaintiffs would have to file a dispute. The CSR also insisted that the dispute form could only come via USPS mail, and Plaintiffs would have to wait to receive the form, which unnecessarily and, on information and belief, intentionally delayed resolution of the dispute.

32. On June 24, 2020, Plaintiffs received the dispute form and immediately faxed the completed form to the number provided by First Data. Plaintiffs included all necessary information, including but not limited to (1) explaining that the card had been stolen and that it was reported stolen on May 31, 2020, and (2) attesting that the specific transactions transferring funds from the card were not authorized by Plaintiffs.

33. The dispute form provided permitted return by fax or email. The email provided in the dispute form was an email address at firstdata.com, confirming that First Data (not any subsidiary) was responsible and directly involved in managing and making decisions relating to the card account at issue.

34. On July 9, 2020, after providing 10 business days for First Data to act in accordance with the law after receiving the dispute form, Plaintiffs still had not received a reversal of the disputed charges or any correspondence relating to the dispute.

35. Given the failure to respond or act, Plaintiffs again called the customer service number on July 9, 2020. During that call, the CSR informed Plaintiffs that the dispute had been denied on July 2, 2020. The CSR explained that the dispute was denied because First Data claimed that the money had gone to the intended recipient (or words to that effect). Plaintiffs explained that the unauthorized transfers were a case of fraud, so it would be impossible for First Data to have reached that conclusion. The CSR agreed and could not offer **any** explanation for the conclusion.

36. During that same call, Plaintiffs requested to speak to a manager. The manager was also incapable of offering any explanation for First Data's purported determination. Plaintiffs reiterated that they did not make or authorize the transfers, nor are Plaintiffs associated with the Chime bank account where the funds were transferred (or any other Chime bank account, for that matter). Plaintiffs asserted that no one could, in good faith, have reached the conclusion that First Data claimed it had reached. The manager offered no additional explanation and stated that the only option was to file an appeal. The manager stated that the firstdata.com email address provided in prior correspondence was an acceptable way to initiate an appeal. At that time, Plaintiffs stated their intent to file an appeal, but also their intent to file a lawsuit if this matter was not resolved promptly.

37. On July 9, 2020, the same day of the call discussed immediately above, Plaintiffs sent a fax and an email to the firstdata.com email address provided in prior correspondence and notified First Data of the appeal request, as well as the intent to file a lawsuit if the matter was

not resolved promptly. In that correspondence, Plaintiffs again described the facts relating to the situation in detail, attested that the transfers at issue were fraudulent, and notified First Data of its violations of Federal law. To date, Plaintiffs have received no response to this correspondence.

38. On July 13, 2020, Plaintiffs received via US Mail the written denial of the dispute filed on June 24, 2020. Although the fact of that denial had been communicated orally on July 9, 2020, the written denial dated July 2, 2020, specifically stated, "We have completed our investigation of the dispute on your card and have determined that no error occurred. The dispute claim has been denied and your dispute claim has been closed. You have the right to request copies of the documents that we utilized to make this determination." The foregoing is the entirety of results of the "investigation" reports to Plaintiffs.

39. The July 2, 2020 written denial did not acknowledge the claim of fraud, nor did it provide any details addressing the substance of the dispute.

40. On information and belief, the July 2, 2020 written denial is a form letter that was routinely issued without any legitimate investigation into the facts of the dispute.

41. Based at least on the firstdata.com email address specified to be used to submit the original dispute form, First Data personnel issued the denial form.

42. On July 13, 2020, Plaintiffs sent an email to the provided firstdata.com email address referencing the July 2, 2020 determination, quoting the language stating the right to request underlying documents included therein, and requesting that any documents utilized to make the determination be provided immediately.

43. On July 16, 2020, Plaintiffs again called the EIP Card customer service number to determine the status of this matter as well as when Plaintiffs would receive the requested

documents. During that call, the CSR asked for any reference numbers provided by law enforcement relating to the mail theft, including the EIP Card. That same day, Plaintiffs sent an email to the firstdata.com email address providing the USPS case number and explaining that the FBI had not provided Plaintiffs with a reference number when Plaintiffs reported the theft to the FBI. Plaintiffs then followed up with another email later that same day after speaking with the FBI, explaining that the FBI did not have a reference number and that the FBI had stated that the USPS would be handling the investigation. Plaintiffs provided the contact number for the FBI to permit First Data to verify this information. Also, Plaintiffs provided another USPS case number pertaining specifically to theft from Plaintiffs' mailbox (as opposed to the general report relating to all neighborhoods previously filed by one of Plaintiffs' neighbors).

44. On July 16, 2020, Plaintiffs, in the first of the emails discussed immediately above, noted that no documents had been provided in response to the July 13 request and reiterated the request for any documents utilized to make the determination.

45. To date, no documents "utilized to make [the July 2] determination" have been provided by First Data.

46. Based on the failure to provide any documents in response to Plaintiffs' requests, there were no documents used to make the determination.

47. Based on content of the July 2 denial letter (or lack thereof) and failure to provide any supporting documentation to Plaintiffs, First Data has no evidence to support its stated conclusion that the June 2 and 3 transfers were not in "error" and not unauthorized transfers.

48. On or about July 20, 2020, Plaintiffs received another dispute form dated July 10, 2020 from First Data concerning the same transactions for which Plaintiffs had already

provided a completed dispute form on June 24, 2020. In response, Plaintiffs sent an email on July 20, 2020 to the firstdata.com email address referencing the July 10, 2020 dispute form, referring First Data to the prior completed dispute form and correspondence, and requesting in bold, highlighted text that First Data immediately contact Plaintiffs if any additional information was needed.

49. Plaintiffs received no response to the July 20, 2020 email.

50. On August 17, 2020, Plaintiffs received an additional dispute denial letter dated August 7, 2020 from First Data.

51. The body of the August 7, 2020 denial letter is identical to the body of the July 2, 2020 denial letter.

52. To date, Plaintiffs have received no response from First Data relating to their July 9, 2020 Appeal Notice.

COUNT I
(Violations of Electronic Funds Transfer Act)

53. Plaintiffs incorporate the above paragraphs herein by reference.

54. This is a claim asserted against Defendant for violation of the federal Electronic Funds Transfer Act 15 U.S.C. §§ 1693 et seq. (the "EFTA").

55. Each Plaintiff is a “consumer” as defined in 15 U.S.C. § 1639a(6).

56. Defendant is a “financial institution as that term is defined in 15 U.S.C. § 1639a(9).

57. The transactions which extracted funds from Plaintiffs’ EIP Card account on June 2 and 3 without Plaintiffs’ knowledge or authority were each “unauthorized electronic fund transfer” as that term is defined in 15 U.S.C. § 1639a(12) and constitute an “error” within the meaning of 15 U.S.C. § 1693f(f).

58. Further, Plaintiffs reported the EIP Card that was issued by Defendant stolen on May 31, 2020 and asked to have the account frozen or otherwise disabled before any unauthorized electronic fund transfers had occurred. Despite this and in violation of the EFTA, Defendant failed to freeze or disable the account.

59. But/for Defendant's failure to freeze the account, the June 2 and 3 unauthorized electronic fund transfers would not have occurred, and Defendant's failure is a direct and proximate cause of Plaintiffs' loss.

60. The same day after learning of the unauthorized electronic fund transfers, Plaintiffs provided prompt and reasonable notice to Defendant of the unauthorized transactions that occurred on June 2 and 3. Plaintiffs notice constitutes notification of error within the meaning of 15 U.S.C. § 1693f(a).

61. Pursuant 15 U.S.C. § 1693g, Plaintiffs are not liable for any of the unauthorized charges both because of the notice provided on May 31, 2020 that the EIP Card had been stolen and the notice provided on July 9, 2020. Plaintiffs did not initiate, authorize, or know about or benefit from any of the transactions. Moreover, Plaintiffs provided sufficient information to Defendant to establish that Plaintiffs were not liable for the unauthorized charges, and Defendant has not met and cannot meet its burden under 15 U.S.C. § 1693g(b) of establishing that the charges were authorized.

62. Defendant has violated and continues to violate the EFTA by failing to provide credit for the unauthorized transactions.

63. Defendant also violated the EFTA by failing to timely and reasonably investigate Plaintiffs' notification of error, by failing to provide adequate written response to that notification and by and failing, upon receipt of that notification, to provide credit for the

unauthorized electronic transfers as required by 15 U.S.C. § 1693f. Defendant did not conduct any reasonable or good faith investigation and had no reasonable basis for its belief or position that the charges reported by Plaintiff as unauthorized were in fact authorized, valid and not in error.

64. Defendant knowingly and willfully concluded that the charges were not in error knowing that such conclusion could not reasonably have been drawn from the evidence available to Defendant at the time of its investigation.

65. The acts and omissions made by Defendant in violation of the EFTA occurred within one year of the filing prior to this action.

66. On information and belief, Defendant's acts and omissions in responding to the unauthorized charges reported by Plaintiffs were in accordance with its standard procedure for handling such matters, which constitutes a pattern and practice of violating the EFTA in responding to reports of unauthorized transactions.

67. As a proximate result of Defendant's violations of the EFTA, Plaintiffs have suffered actual damages, including loss of funds and loss of access to funds, among other things.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests the Court enter judgment against Defendant declaring that Defendant violation the EFTA and awarding Plaintiffs:

1. Actual damages;
2. Statutory damages pursuant to 15 U.S.C. § 1693m;
3. Treble damages pursuant to 15 U.S.C. § 1693f(e);
4. Costs and reasonable attorneys' fees pursuant to 15 U.S.C. § 1693m(a)(3) as well as expenses and interest; and

5. Such other and further relief as this Court deems just and proper.

JURY DEMAND

Plaintiff demands trial by jury under Fed. R. Civ. P. 38.

Dated: August 18, 2020

Respectfully Submitted

/s/ Andrew John Fossum

Andrew John Fossum
Texas State Bar No. 24084918
andrew.fossum@spearheadlegal.com

SPEARHEAD LEGAL LLP
620 Newport Center Dr., Suite 1100
Newport Beach, CA 92660
Phone: (512) 253-2166
Fax: (949) 409-8383

ATTORNEY FOR PLAINTIFFS